POSITIVE TECHNOLOGIES

ЗАО «ПОЗИТИВ ТЕКНОЛОДЖИЗ»
107061, МОСКВА, ПРЕОБРАЖЕНСКАЯ ПЛ., Д. 8
ТЕЛ. +7 495 744-01-44, ФАКС +7 495 744-01-87, PT@PTSECURITY.COM
PTSECURITY.RU, MAXPATROL.RU, SECURITYLAB.RU

СИСТЕМА СКАНИРОВАНИЯ ФАЙЛОВ MULTISCANNER

РУКОВОДСТВО ПО УСТАНОВКЕ

ОГЛАВЛЕНИЕ

1. Введение

PT MultiScanner – это система, которая позволяет проводить сканирование файлов набором антивирусных программ и получать результаты сканирования в виде отчета. С помощью этого автоматизированного сервиса клиент может рассчитать достоверную оценку опасности, исходящей от файлов, получаемых извне информационной системы.

1.1. Принцип работы

Пользователь предоставляет системе один или несколько файлов. PT MultiScanner обрабатывает полученные файлы и собирает результаты работы всех антивирусных программ с полученным набором файлов. В отчет также включается текущая версия антивирусной программы и ее базы знаний. Для каждого файла система вычисляет хеш, который позволяет идентифицировать и получить результаты сканирования файла без пересканирования, если такие результаты уже хранятся в системе.

2. Поддерживаемые операционные системы

Система PT MultiScanner поддерживает установку на Ubuntu 14.04 x64, а также следующие системы для агентов:

- Windows x64 x86 (NT 6.1 +)
- Ubuntu 10.04 x64
- Ubuntu 12.04 x64
- CentOS 7 x64

Для установки можно использовать следующие внешние ресурсы:

- Репозитории

- Ubuntu 10.04

```
deb http://ru.archive.ubuntu.com/ubuntu/ lucid main universe
deb http://ppa.launchpad.net/fkrull/deadsnakes/ubuntu lucid main
```

- Ubuntu 14.04

```
deb http://ru.archive.ubuntu.com/ubuntu/ trusty main universe
```

- CentOS 7

```
http://mirror.centos.org/centos/7/os/x86_64/
http://download.fedoraproject.org/pub/epel/7/x86_64/
http://dl.iuscommunity.org/pub/ius/stable/CentOS/7/x86_64/
```

- Если доступ в интернет организован через прокси, то настройте прокси:

Ubuntu:

```
http://help.ubuntu.ru/wiki/%D0%BF%D1%80%D0%BE%D0%BA%D1%81%D0%B8
```

CentOS 7:

```
https://www.centos.org/docs/5/html/yum/sn-yum-proxy-server.html
```

- Если доступ через интернет невозможен, создайте зеркала:

Ubuntu:

```
http://help.ubuntu.ru/wiki/apt-mirror
http://help.ubuntu.ru/wiki/
%D1%81%D0%BE%D0%B7%D0%B4%D0%B0%D0%BD%D0%B8%D0%B5_%D0%B7%D0%B5%D1%80%D0%BA%D
0%B0%D0%BB%D0%B0_%D1%80%D0%B5%D0%BF%D0%BE%D0%B7%D0%B8%D1%82%D0%BE%D1%80%D0%
B8%D1%8F
```

CentOS:

```
http://shurshun.ru/sozdaem-lokalnoe-zerkalo-repozitoriev/
```

- Для скачивания зависимостей (/srv/salt/prepare.sh) нужен доступ к https://pypi.python.org или https://www.python.org.

- доступ в интернет организован через прокси:

воспользуйтесь командой help утилиты,

- доступ в интернет невозможен:

скачайте зависимости и создайте новый архив:

```
cd /srv
tar -czf /tmp/multiscanner-offline-<версия>.tar.gz ./salt/ ./pillar/
```

Внимание! Для стабильной работы узлы должны иметь уникальное имя, не совпадающее с идентификатором minion.

Внимание! Убедитесь, что при перезапуске первым запускается файловый сервер.

3. Подготовка к установке PT MultiScanner

Для того чтобы установить PT MultiScanner, убедитесь, что существует набор серверов (роли можно совмещать):

- для баз данных,
- для RabbitMQ,
- для веб-системы сервера,
- для salt-master,
- для хранения скаченных файлов,
- для агентов (адаптеров антивирусных движков),
- для сервера лицензий с подключенным к ним ключем,
- для дополнительных сервисов.

Кроме того, на сервере для развертывания должен быть развернут salt-master, и на всех серверах — salt-minion.

4. Установка salt-master

Для установки salt-master:

Установить пакеты.

```
wget -O - https://repo.saltstack.com/apt/ubuntu/14.04/amd64/2015.8/SALTSTACK-GPG-KEY.pub | sudo apt-key add -
add-apt-repository 'deb http://repo.saltstack.com/apt/ubuntu/14.04/amd64/2015.8 trusty main'
apt-get update
apt-get install salt-master
```

Запустить мастер.

```
service salt-master restart
```

Подключить minion-salt.

5. Установка minion-salt

Для установки minion-salt на Windows:

- установить Microsoft Visual C++ 2008 SP1 (x86) или Microsoft Visual C++ 2008 SP1 (x64)
- установить salt-minion версии 2015.8. При установке minion указать IP-адрес мастера.

Для установки minion-salt на Unix:

- установить salt-minion версии 2015.8

- Для Ubuntu 10.04 — 14.04

```
wget -O - https://repo.saltstack.com/apt/ubuntu/14.04/amd64/2015.8/SALTSTACK-GPG-KEY.pub | sudo apt-key add -
add-apt-repository 'deb http://repo.saltstack.com/apt/ubuntu/14.04/amd64/2015.8 trusty main'
apt-get update
apt-get install salt-minion
```

- Для CentOS 7

```
rpm --import https://repo.saltstack.com/yum/redhat/7/x86_64/2015.8/SALTSTACK-GPG-KEY.pub
echo "[saltstack-repo]\nname=SaltStack repo for RHEL/CentOS $releasever\nbaseurl=https://repo.saltstack.com/yum/redhat/$releasever/$basearch/2015.8\nenabled=1\ngpgcheck=1\ngpgkey=https://repo.saltstack.com/yum/redhat/$releasever/$basearch/2015.8/SALTSTACK-GPG-KEY.pub" > /etc/yum.repos.d/saltstack.repo

yum install salt-minion
systemctl enable salt-minion
systemctl start salt-minion
```

- Отредактировать конфигурационный файл sudo vim /etc/salt/minion

```
vim /etc/salt/minion
```

Затем заменить мастера, раскомментировав строку “master: salt” и указав IP-адрес мастера вместо “salt”, например master: 10.120.4.37

- Перезапустить агент

- Ubuntu 10.04 - 14.04

```
service salt-minion restart
```

- CentOS 7

```
systemctl restart salt-minion
```

Подтвердить агента на мастере:

```
salt-key -A
```

6. Роли salt

Определены следующие роли salt:

- nginx устанавливает frontend (linux), (обязателен);
- background устанавливает обработчик асинхронных задач. (linux)(обязателен)
- notify - модуль отправки нотификаций. (linux)(обязателен)
- icap - ICAP-интерфейс. (linux)
- smtp - SMTP-интерфейс. (linux)

- background-beat должен существовать в одном экземпляре, запускает периодические задачи. (linux) (обязателен)
- suricata устанавливается на сервере с suricata. (linux)
- agents устанавливает адаптер(linux, windows) (обязателен)
- files - для сканирования файловой шары
- agent-async - требуется для связки с HoneyPot

Пример:

```
grains:
  roles:
    - nginx
    - background
    - background-beat
    - agents
    - files
```

7. Назначение ролей

Назначение ролей выполняется с Salt-Master.

- Просмотр установленных ролей

```
salt '*' -v grains.item roles
```

- Добавление роли

```
salt '<minion id>' -v grains.append roles '<role>'
## например так (имя minion и роль вводится без скобок):
salt 'ms-host' -v grains.append roles 'background'
```

- Удаление роли

```
salt '<minion id>' -v grains.remove roles '<role>'
```

8. Лицензирование

- Выбрать сервер для роли сервера лицензи й(может быть совмещен с другими серверами), например Ubuntu 14.04 x64.
- Вставить или пробросить ключ на этот сервер.
- Установить salt-minion.
- В конфигурационном файле pillar записать IP-адрес сервера лицензий в guardant.ip_name.
- Затем установить на этот сервер будет необходимые приложения.

Внимание! PT MultiScanner не работает при выключенном сервере лицензий или если к нему не подключен ключ.

После каждого подключения (передоключения) ключа нужно перезапустить сервер лицензий.

```
sudo service glds restart
```

9. Процедура развертывания

- Скопировать дистрибутив на salt-master
- Зайти на salt-master.
- заменить Salt State

Внимание! до выполнения команды, указанной ниже, сделайте резервные копии файлов конфигурации. При обновлении версии эти файлы перезаписываются, если происходит обновление.

```
tar -x -f <путь до архива> --directory=/srv --recursive-unlink
```

- Скачать зависимости (для прокси - посмотреть команду help)

```
apt-get update
apt-get upgrade
/srv/salt/prepare.sh --clean
```

Если установка происходит без доступа к интернету (с версии 0.8.0)

- выполняем пункт 3 на Ubuntu 14.04 x64 с доступом к интернету
- переносим файл ms_req.tar.gz на машину с salt-master и выполняем

```
mkdir -p /tmp/ms_req
tar -xf ms_req.tar.gz --directory=/tmp/ms_req --recursive-unlink
/srv/salt/prepare.sh --no-index --find-links /tmp/ms_req
```

- Актуализировать и настроить Pillar

```
vim /srv/pillar/config.sls
```

- Развернуть систему на Linux

```
salt -v -G 'kernel:Linux' pkg.refresh_db   # обновление репозиториев
salt -v -G 'kernel:Linux' pkg.upgrade      # Обновление пакетов
salt -v -G 'kernel:Linux' state.highstate --state-output=mixed
```

- Развернуть агенты на Windows

```
salt-run winrepo.genrepo  # генерация репозитория для винды
salt -v -G 'kernel:Windows' pkg.refresh_db   # обновление репозиториев
salt -v -G 'kernel:Windows' state.highstate --state-output=mixed --
timeout=300
```

Внимание! Если при развертывании возникает ошибка pyvenv-3.4: command not found, то установите пакет python3.4-venv на этот узел.

Positive Technologies — лидер европейского рынка систем анализа защищенности и соответствия стандартам. Компания входит в число наиболее динамично развивающихся участников российской IT-отрасли, демонстрируя ежегодный рост более 50%. Офисы и представительства Positive Technologies расположены в Москве, Лондоне, Риме, Сеуле и Тунисе.

Разработанные экспертами компании программные продукты заслужили международное признание в сфере практической информационной безопасности.

Продукты

Система контроля защищенности и соответствия стандартам MaxPatrol помогает обеспечивать безопасность корпоративных информационных систем и формировать комплексное представление о реальном уровне защищенности IT-инфраструктуры организации. Система позволяет контролировать выполнение требований государственных, отраслевых и международных стандартов, таких как Федеральный закон № 152-ФЗ «О персональных данных», СТО БР ИББС, ISO 27001/27002, SOX 404, PCI DSS. В MaxPatrol объединены активные механизмы оценки защищенности, включая функции системных проверок, тестирования на проникновение, контроля соответствия стандартам — в сочетании с поддержкой анализа различных операционных систем, СУБД и веб-приложений.

Система анализа защищенности XSpider более 10 лет является признанным лидером среди средств сетевого аудита ИБ. На сегодняшний день это один из лучших интеллектуальных сканеров безопасности в мире. Более 1000 международных компаний успешно используют XSpider для анализа и контроля защищенности корпоративных ресурсов.

Услуги

Компания Positive Technologies специализируется на проведении комплексного аудита информационной безопасности, на оценке защищенности прикладных систем и веб-приложений, тестировании на проникновение и внедрении процессов мониторинга информационной безопасности. Статус PCI DSS Approved Scanning Vendor позволяет проводить работы по проверке соответствия данному стандарту.

Клиенты

В числе заказчиков Positive Technologies — более 1000 государственных учреждений, финансовых организаций, телекоммуникационных и розничных компаний, промышленных предприятий России, стран СНГ и Балтии, а также Великобритании, Германии, Голландии, Израиля, Ирана, Китая, Мексики, США, Таиланда, Турции, Эквадора, ЮАР и Японии.

Вклад в индустрию

Принимая активное участие в развитии IT-отрасли, Positive Technologies выступает организатором международного форума по информационной безопасности Positive Hack Days и развивает SecurityLab.ru — самый популярный ИБ-портал на русском языке.

Более подробную информацию можно получить на сайте www.ptsecurity.ru